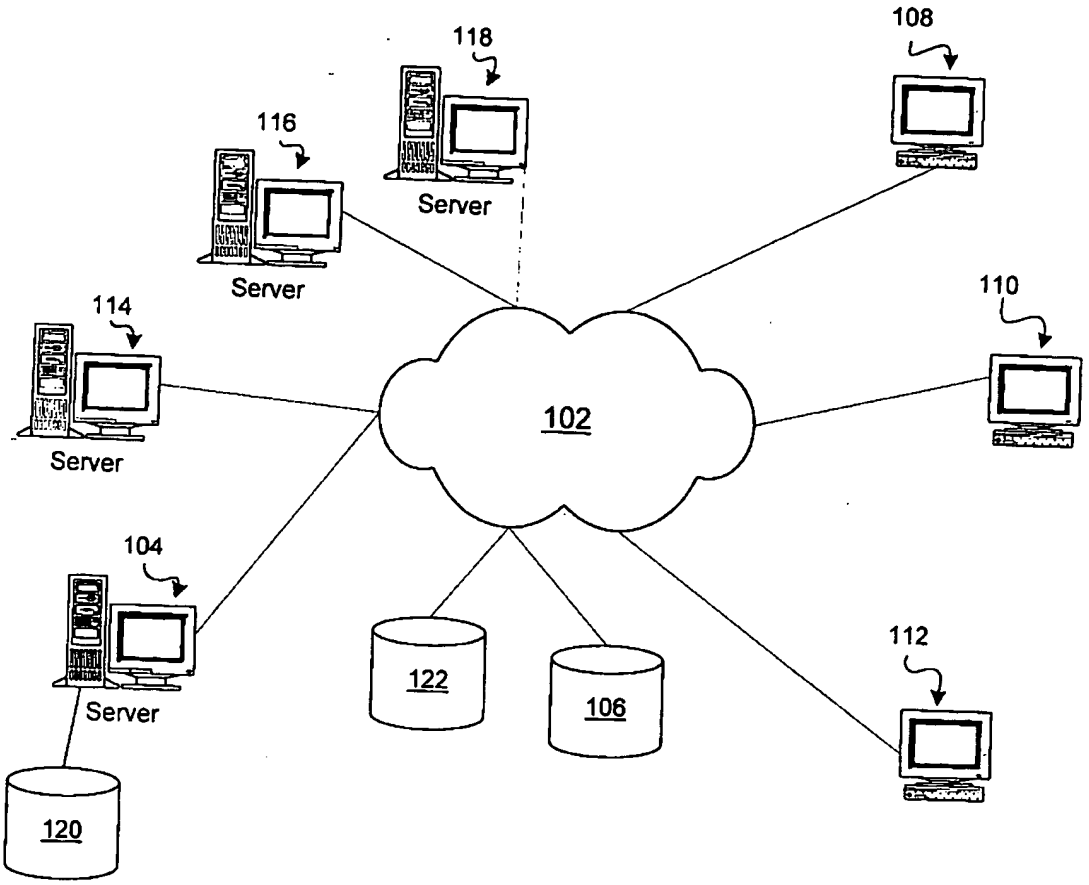
EJ187645716US

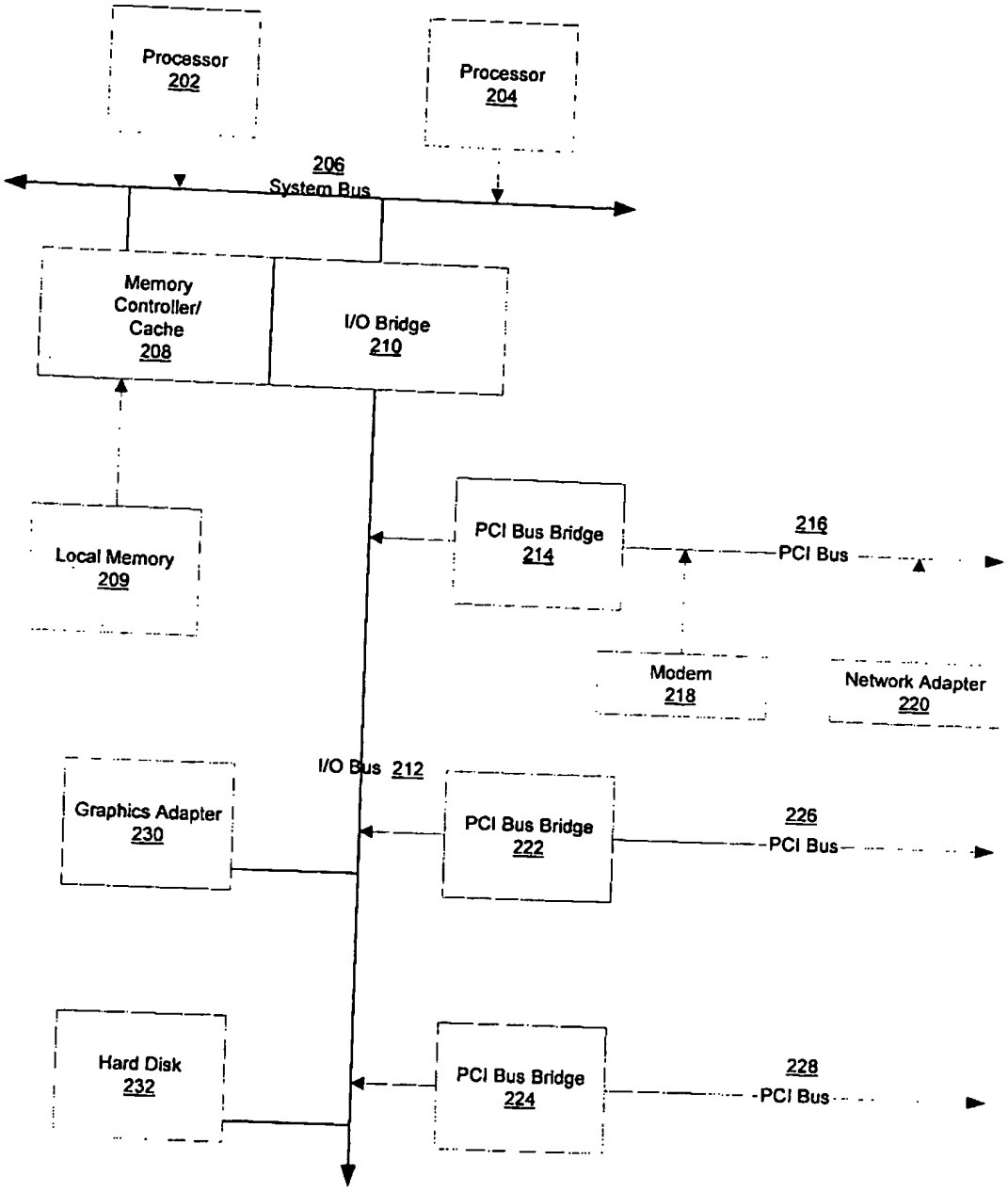


100

Network

Figure 1

09/09/2004, 09:09:09



200

Figure 2

AUS990800US1

```
Attribute ::= SEQUENCE {
        type AttributeType,
        values SET OF AttributeValue
}

AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY type
```

Figure 3

ASN.1 Notation of the X.500
Attribute data type
AUS990800US1

```
400 →
    EmailAddress = SEQUENCE {                    ← 402
            1.2.840.113459.1.9.1,
            "javauser@acme.com", "javauser@someisp.net"
    }
            ↑ 404                                ↑ 406
408 →
    ContentType = SEQUENCE {                     ← 410
            1.2.840.113459.1.9.3,
            1.2.840.113459.1.7.2
    }
            ↑ 412
```

Figure 4

Attributes EmailAddress and
ContentType using PKCS9
AUS990800US1

EmailAddress 502

```
30 36 06 09 2A 86 48 86  F7 0D 01 09 01 31 29 16
11 6A 61 76 61 75 73 65  72 40 61 63 6D 65 2E 63
6F 6D 16 14 6A 61 76 61  75 73 65 72 40 73 6F 6D
65 69 73 70 2E 6E 65 74
```

ContentType 504

```
30 18 06 09 2A 86 48 86  F7 0D 01 09 03 31 0B 06
09 2A 86 48 86 F6 33 01  07 02
```

Figure 5

DER Encoding of EmailAddress
and ContentType Attributes
AUS990800US1

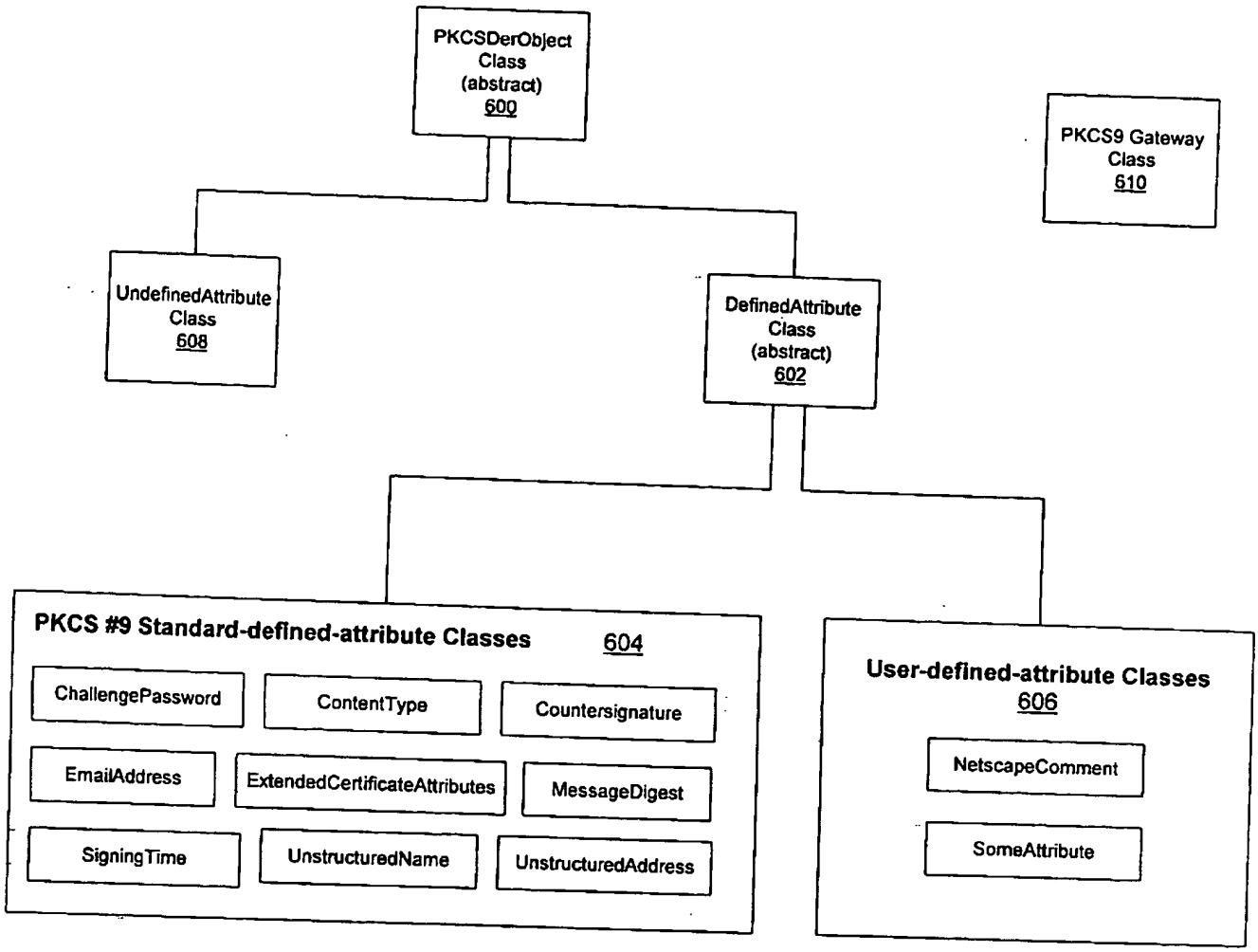


Figure 6

Attribute Classes and Hierarchy

AUS990800US1

Figure 7A
Requesting an Attribute Object via the PKCS9 class
AUS990800US1

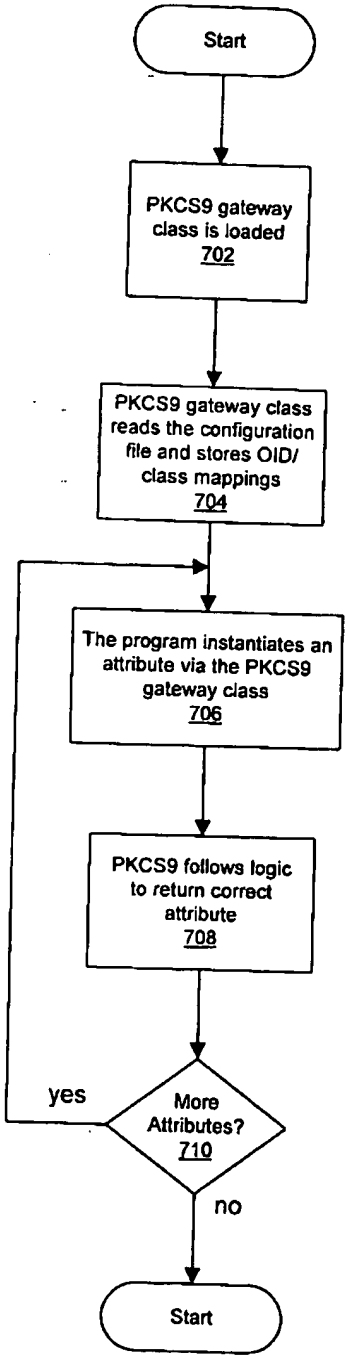


Figure 7B
Configuration File
AUS990800US1

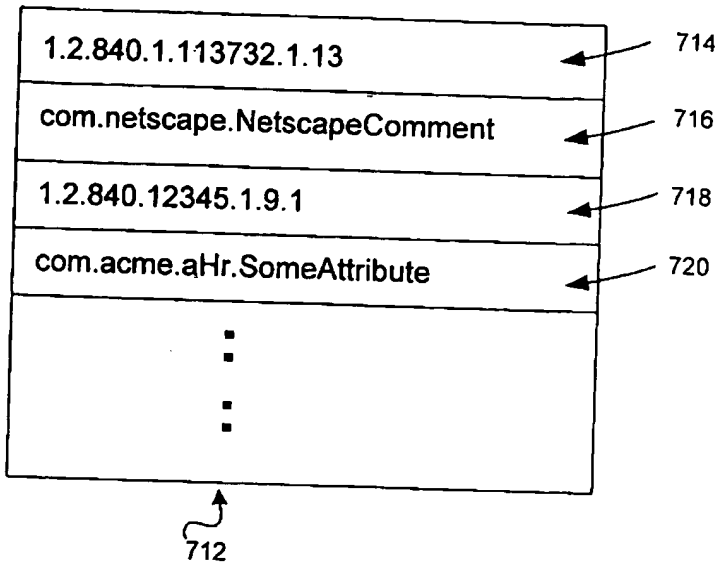


Figure 7C
Attribute Mapping
AUS990800US1

Object Identifier	Class
1.2.840.113549.1.9.1	EmailAddress
1.2.840.113549.1.9.2	UnstructuredName
1.2.840.113549.1.9.3	ContentType
1.2.840.113549.1.9.4	MessageDigest
1.2.840.113549.1.9.5	SigningTime
1.2.840.113549.1.9.6	Countersignature
1.2.840.113549.1.9.7	ChallengePassword
1.2.840.113549.1.9.8	UnstructuredAddress
1.2.840.113549.1.9.9	ExtendedCertificateAttributes
1.2.840.1.113732.1.13	com.netscape.NetscapeComment
1.2.840.12345.1.9.1	com.acme.aHr.SomeAttribute
:	:

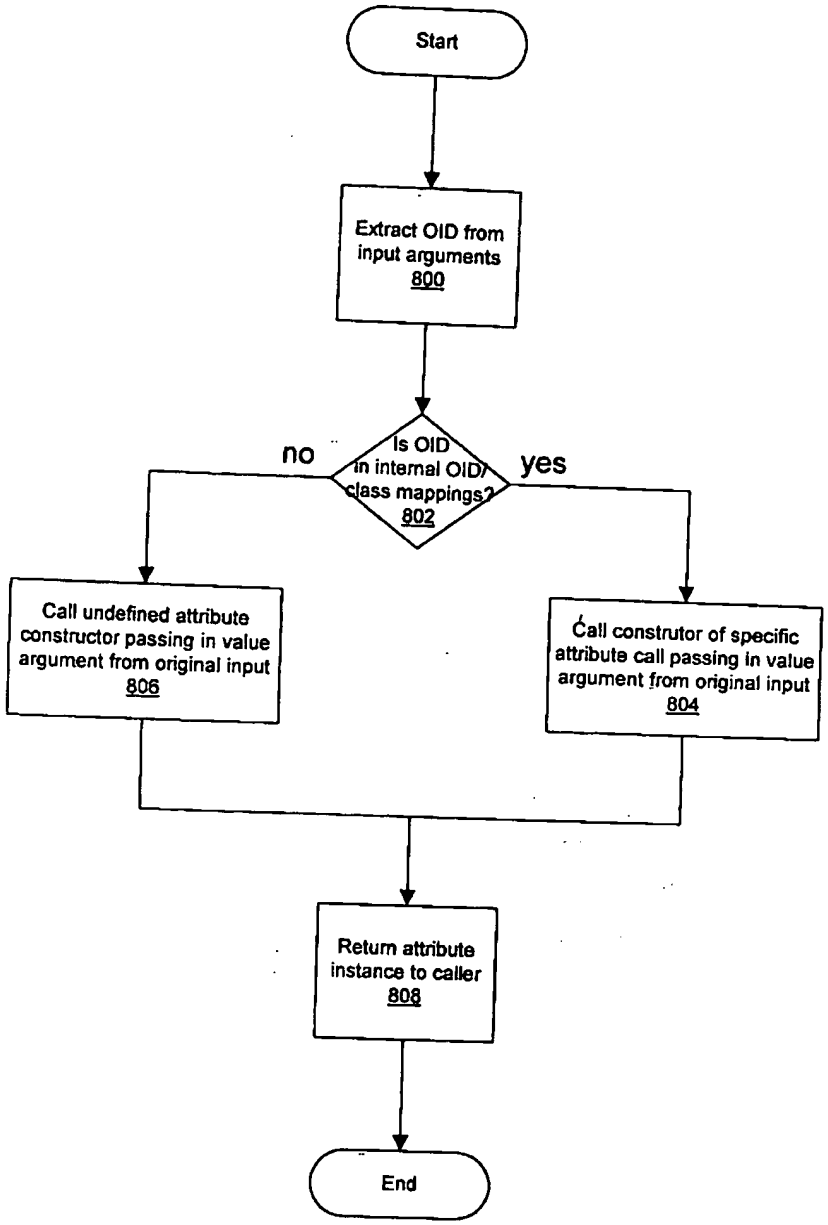


Figure 8

Logic of getAttribute() method for PKCS9

AUS990800US1